

- 4) Establishes the University of California (UC), the California State University (CSU), and the California Community Colleges (CCC) as the three segments of public postsecondary education in the state, as specified.
- 5) Requests the Trustees of the CSU, the Regents of the UC, and the governing board of each community college district to allow the faculty, staff, and students to identify their sexual orientation, gender identity, and gender expression on any forms used to collect specified demographic data and to report that data, as specified.

This bill:

- 1) Prohibits information pertaining to SOGISC collected pursuant to existing law from being disclosed in personally identifiable form to any entity outside of California state government, or a vendor contracted to provide services to the state, except if either of the following apply:
 - a) Pursuant to a contract or data sharing agreement where the reporting SOGISC elements is an explicit and mandatory condition for participation in a federal or interstate program or survey.
 - b) Pursuant to a subpoena or warrant that is valid and enforceable in California.
- 2) Limits the information pertaining to SOGISC reported in an identifiable form to the minimal extent required to meet the applicable exception, and in compliance with the Information Practices Act of 1977, as specified.
- 3) Provides that any person who commits a violation of this bill shall be subject to existing penalties established by the Information Practices Act of 1977, as specified.
- 4) Provides that information collected by the UC, CSU, or CCCs pursuant to existing law is subject to the disclosure restrictions established by this bill and existing penalties, as specified.
- 5) Defines “information pertaining to SOGISC” to mean information pertaining to any of the following:
 - a) A person’s sexual orientation identity.
 - b) A person’s gender identity or gender expression.

- c) A person's identification as intersex, or identification as possessing sex characteristics that vary from those typically associated with a person's sex assigned at birth.
 - d) Information pertaining to SOGISC also includes information that could reasonably be used to infer a person's transgender or intersex status, as specified.
- 6) Provides that the provisions of this bill are severable. If any provision of this bill or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application.
- 7) Provides that no reimbursement is required by this bill for a specified reason.

Background

Author Statement. According to the author's office, "SB 1114 protects LGBTQ+ Californians from discrimination and harm by strengthening privacy protections for highly sensitive data related to [SOGISC]. The bill restricts California state agencies from sharing SOGISC data outside state government and limits disclosure to narrow circumstances."

Further, "inclusive data collection helps California state agencies better serve diverse communities. But as hostility from the federal government toward communities of color, immigrants, and LGBTQ+ people has grown, so has the need to ensure sensitive information cannot be misused. Federal agencies have increasingly sought expanded access to state-held data, often framed as efforts to reduce fraud, waste, and abuse. While many recent examples involve requests for immigration or health data, they underscore why clear guardrails on data sharing are essential. Similar to other sensitive information the state collects, SOGISC data should be protected with strong limitations on when and how it can be shared outside of California state government, especially given the demonstrated hostility of the Trump administration toward LGBTQ+ communities."

The LGBTI Disparities Reduction Act. Established by AB 959 (Chiu, Chapter 565, Statutes of 2015), the LGBTI Disparities Reduction Act (Act) was intended to reduce health and well-being disparities for LGBTI communities by ensuring that sexual orientation and gender identity data is collected on a statewide basis by key government agencies that deal with health and human services.

According to the Senate Floor analysis of that bill at the time, “[s]tate government agencies routinely collect demographic data on race, ethnicity, gender, and disability on a wide variety of state forms and surveys. The purpose of this data is to help better understand disparities in underserved communities. Current law only requires any state agency, board, or commission that directly, or by contract, collects demographic data to separate the collection of this data by major Asian groups. The law is silent on demographic data collection based on sexual orientation or gender identity.”

Since 2015, the Act has been amended to, among other things, expand the list of state entities required to collect voluntary self-identification information on SOGISC to include various education and employment-related agencies; expand the list of state entities to include the Department of State Hospitals (DHS), the Department of Rehabilitation (DOR), the Department of Developmental Services (DDS), and the Department of Community Services and Development (DCSD); and to require, rather than permit, DPH to collect demographic data, including SOGISC data from third parties on any forms or electronic data systems, as specified.

As noted in previous Senate analyses on the topic, LGBTI communities face disproportionately high rates of poverty, suicide, homelessness, isolation, substance abuse, and violence, and low rates of health insurance. These issues are more prevalent for youth and seniors, communities of color, and transgender and undocumented communities. Supporters state that collecting voluntary data on sexual orientation and gender identity is a necessary first step to understand the extent to which LGBTI communities are experiencing disparities and whether government programs are effectively reaching LGBTI individuals in need of care and assistance.

Rapidly Changing Data Landscape. According to the [State Health Access Data Assistance Center](#), sex (i.e., male, female) has been collected on various types of surveys for many years, dating back to the first iteration of the census in 1790. However, collection of detailed sexual orientation and gender identity data is a relatively new endeavor for many federal and state agencies. The Center further notes that, “[s]ince the beginning of 2025, the landscape of [SOGISC] data collection has shifted again, marking a departure from previous federal policy. Following the rescission of the Biden Administration’s EO 14075, which had previously expanded [SOGISC] data collection efforts, a new Executive Order No 14168 (2025), titled *Defending Women From Gender Ideology Extremism and Restoring Biological Truth to the Federal Government*, redefines how federal agencies approach sex and gender identity data.”

The Center states that nearly 14 million adults in the United States identify as part of the LGBT community – more than the entire population of Pennsylvania. While research is limited, studies continually find that LGBT people are more likely to experience health, economic, and social disparities than non-LGBT peers.

Additionally, the author of this bill argues that federal agencies have increasingly sought expanded access to state-held data, often framed as efforts to reduce fraud, waste, and abuse. The author’s office states that, for example, “the U.S. Department of Agriculture has sought unprecedented access to detailed data, including information about immigration status, from state Supplemental Nutrition Assistance Program (SNAP) systems and their contractors, while the Centers for Medicare & Medicaid Services (CMS) has shared immigration information about Medicaid enrollees with the Department of Homeland Security.”

Further compounding the emerging data sharing problem, recent news reports have identified instances of government data handled by the federal Department of Government Efficiency (DOGE) being compromised and potentially disseminated. A March 11, 2026 article in the *Washington Post* titled “[Whistleblower claims ex-DOGE member says he took Social Security data to new job](#),” the Social Security Administration’s (SSA) internal watchdog is investigating a complaint alleging “a former U.S. DOGE Service employee claimed he had access to two highly sensitive agency databases and planned to share the information with his private employer – a claim that, if true, would constitute an unprecedented breach of security protocols at an agency that services more than 70 million Americans.”

In response to this, Ranking Member of the House Committee on Oversight and Government Reform, Rep. Robert Garcia of Long Beach, recently expanded an investigation of DOGE-related data leaks at the SSA after reporting indicated “a former employee of Elon Musk’s [DOGE] remains in possession of Americans’ personally identifiable Social Security information on a personal device and may also have the ability to remotely manipulate millions of Americans’ Social Security data.”

Access to data as artificial intelligence (AI) is rapidly improving is becoming increasingly valuable. Coined by the British mathematician Clive Humby in 2006, the phrase “data is the new oil” is intended to signify that raw data, like crude oil, is immensely valuable but useless until refined, processed, and analyzed. Today, the federal government has broad access to and utilization of some of the most advanced technology ever created. Examples include Palantir Technologies, a Silicon Valley data-analytics company that builds software used by intelligence and law-enforcement agencies. Reporting shows that the federal government has

explored using Palantir's Foundry platform to combine data from multiple agencies such as Health and Human Services, Social Security, and the Internal Revenue Service. Centralized "data fusion" makes it easier to track individuals across different government systems, while AI can quickly automate the process of identifying patterns and behaviors.

History of Government Targeting the LGBTQI Community. The "Lavender Scare" of the 1940s-1960s was a time of intentional and malicious targeting of the LGBTQI community by the federal government under the premise that queer individuals posed a security threat to the country because they could be blackmailed by foreign governments. In 1953, Executive Order 104450 formally barred "sexual perversion" (the term used at the time to describe the LGBTQI community) from federal employment. Federal agencies were tasked with actively investigating employees' private lives to identify gay people and as a result thousands of federal workers were fired, forced to resign, or publicly outed. Investigations often involved interrogations, surveillance, and pressure to reveal others who might also be gay.

During the mid-20th century, federal law enforcement agencies also surveilled LGBTQ organizations including monitoring groups such as the Mattachine Society, one of the earliest gay rights organizations, and collecting intelligence files on individuals suspected of homosexuality or "sexual deviance." The purpose of this monitoring was often political in nature or to intimidate an individual or the LGBTQ community, rather than criminal investigations.

Complicating things further, a 2018 report from the Stanford Graduate School of Business titled "[Deep Neural Networks Are More Accurate than Humans at Detecting Sexual Orientation from Facial Images](#)," claimed that AI could distinguish between gay and heterosexual men with about 81% accuracy from a single photo and about 74% for women. The system used facial features extracted by a deep neural network from over 35,000 images. The study triggered major controversy from critics warning such technology could be dangerous if used for surveillance or discrimination. Many scientists disputed the conclusions and methodology while multiple LGBTQ groups argued it relied on stereotypes rather than biological signals.

Information Practices Act of 1977 Penalties. Among other things, when the Legislature established the Information Practices Act of 1977, it declared that the "right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right to privacy in information pertaining to them."

Further, the Legislature made the following findings, “(a) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies. (b) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information. (c) In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits.”

The Information Practices Act of 1977 provides for penalties for the intentional violation of any provision of this specific law or of any rules or regulations adopted thereunder, by an officer or employee of any agency shall constitute a cause for discipline, including termination of employment. Additionally, the Information Practices Act of 1977 states that any person who willfully requests or obtains any record containing personal information from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000, or imprisoned more than one year, or both.

Finally, the Information Practices Act of 1997 provides that except for disclosures which are otherwise required or permitted by law, the intentional disclosure of medical, psychiatric, or psychological information in violation of the disclosure provisions of that law is punishable as a misdemeanor if the wrongful disclosure results in economic loss or personal injury to the individual to whom the information pertains.

This bill specifies that a violation of this bill is subject to the penalties described under Article 10 (commencing with Section 1798.55) of Chapter 1 of Title 1.8 of Part 4 of Division 3 of the Information Practices Act of 1977 described above.

Protecting Personally Identifiable SOGISC Data. This bill restricts personally identifiable information pertaining to SOGISC data collected pursuant to the LGBTI Disparities Reduction Act from being disclosed to any entity outside of California state government, or a vendor contracted to provide services to the state. Additionally, this bill requires information pertaining to SOGISC reported in an identifiable form be limited to the minimal extent required to meet the applicable exception, and in compliance with the Information Practices Act of 1977.

In support of the bill, the author’s office notes that in 2025, “CMS instructed hospitals participating in federally funded programs to provide data on transgender health care, and subsequently, the Department of Justice issued subpoenas for personally identifiable information of transgender patients to at least 20 hospitals,

many of them public. In practice, these requests can expose sensitive information about individuals and their families and create risks that data collected to administer benefits or provide services could be used for unrelated purposes, such as immigration enforcement or surveillance.”

Prior/Related Legislation

SB 957 (Wiener, Chapter 868, Statutes of 2024) required, rather than permit, DPH to collect demographic data, including SOGISC, and intersexuality data, from third parties on any forms or electronic data systems, unless prohibited by federal or state law, as specified. Added SOGISC to the information reported for the purpose of statewide or local immunization information systems, as specified and requires DPH to prepare an annual report concerning SOGISC data, as specified.

AB 1163 (L. Rivas, Chapter 832, Statutes of 2023) expanded the list of state entities required to collect voluntary self-identification information on SOGISC to include the DSH, the DOR, DDS, and the DCSD.

AB 677 (Chiu, Chapter 744, Statutes of 2017) expanded the list of state entities required to collect voluntary self-identification information on SOGISC to include various education and employment-related agencies.

AB 959 (Chiu, Chapter 565, Statutes of 2015) required the Department of Health Care Services, DPH, DSS, and the Department of Aging to collect voluntary self-identification information on sexual orientation and gender identify, as specified.

FISCAL EFFECT: Appropriation: No Fiscal Com.: Yes Local: Yes

SUPPORT:

Equality California (Source)
California LGBTQ Health and Human Services Network

OPPOSITION:

None received

ARGUMENTS IN SUPPORT: In support of the bill, Equality California writes, in part, “SB 1114 establishes clear guardrails and ensures SOGISC data cannot be disclosed outside of California state government except in limited circumstances – when explicitly required for participation in a federal or interstate program, or in

response to a subpoena or warrant that is valid and enforceable in California. The bill also defines SOGISC to include sexual orientation, gender identity, and variations in sex characteristics, and clarifies that information that could reasonably be used to infer transgender or intersex status is also protected. Finally, SB 1114 extends these protections to SOGISC data collected by public postsecondary education institutions and makes violations subject to existing penalties under the Information Practices Act.”

DUAL REFERRAL: Senate Governmental Organization Committee and Senate Privacy, Data Technology, & Consumer Protection Committee